FINITE FIELDS AND THEIR APPLICATIONS **2,** 173–191 (1996)
ARTICLE NO. 0011

On Lower Bounds for Incomplete Character Sums over Finite Fields

FERRUH ÖZBUDAK

Department of Mathematics, Bilkent University, Ankara 06533, Turkey
E-mail: ozbudak@fen.bilkent.edu.tr

Communicated by Stephen D. Cohen

Received January 17, 1995

The purpose of this paper is to extend results of Stepanov (1980; 1994) about lower bounds for incomplete character sums over a prime finite field F_p to the case of arbitrary finite field F_q. © 1996 Academic Press, Inc.

1. INTRODUCTION

Let $p > 2$ be a prime number, F_p be a prime finite field with p elements which we identify with the set $\{1, 2, \ldots, p\}$. Let $f(x)$ be a polynomial of degree > 1 with coefficients in F_p and define

$$S_p(f) = \sum_{x \in F_p} \left(\frac{f(x)}{p} \right),$$

where (a/p) is Legendre symbol:

$$\left(\frac{a}{p} \right) = \begin{cases} 0 & \text{if } a = 0 \\ 1 & \text{if } a \neq 0 \text{ and } a \text{ is a square in } F_p \\ -1 & \text{if } a \text{ is not a square in } F_p \end{cases}$$

As a consequence of Weil's result [9] we have [3, Section 1.3] that if m is the number of distinct roots of f in its splitting field over F_q, χ is a nontrivial

1071-5797/96 $18.00

multiplicative character of F_q of exponent s, and f is not an sth power of a polynomial, then

$$\left|\sum_{x\in F_q}\chi(f(x))\right| \le (m-1)q^{1/2}.$$

Karatsuba [4] and Mit'kin [7] proved existence of a square-free polynomial in $F_p[x]$ of degree $n \ge 2(p \log 2/\log p + 1)$ for which

$$S_p(f) = \sum_{x=1}^{p}\left(\frac{f(x)}{p}\right) = p.$$

Therefore the Weil estimate cannot be sharpened essentially, for example to

$$\left|\sum_{x\in F_q}\chi(f(x))\right| \le ((m-1)q)^{1/2}.$$

Later Stepanov [8] gave a very simple proof of this result by using the Dirichlet pigeon-hole principle and extended it to the case of incomplete sums

$$S_N = \sum_{x=1}^{N}\left(\frac{f(x)}{p}\right), \qquad 1 \le N \le p.$$

Namely, he proved the existence of a square-free polynomial $f(x) \in F_p[x]$ of degree $\ge 2\,((N+1)\log 2/\log p + 1)$ for which

$$S_N(f) = \sum_{x=1}^{N}\left(\frac{f(x)}{p}\right) = N.$$

In his book [3, Section 2.1.3, problem 15] he has shown that the same method can be used to get similar results for an additive character.

We will prove the following theorem which gives an extension of this result to the case of arbitrary nontrivial multiplicative characters of an arbitrary finite field F_q.

THEOREM 1. *Let $q = p^m$, p a prime number, $B = \{x_1, x_2, \ldots, x_N\} \subseteq F_q$ an arbitrary subset of F_q, and χ a nontrivial multiplicative character of*

F_q. Let $s > 1$ be an exponent of χ. Assume $N = c(q) \log q$ and $n \geq 1$ is an integer satisfying

$$n \geq \frac{N \log s}{\log q} - \frac{N \log(1 - 1/q) + \log(1 - K_q(1 - 1/q)^{-N})}{\log q} + \frac{\log(1 - s^{-N})}{\log q} + R_{N,q}, \tag{1}$$

where

$$0 \leq K_q \leq 5 \log \frac{q}{q-1} \tag{2}$$

and

$$|R_{N,q}| \leq \left(M \frac{\log q}{q} \right)^2 \frac{1}{(1 - 1/q)^N - K_q} \tag{3}$$

and also where:

(i) *if $c(q) \to \infty$ as $q \to \infty$, then $M = e/\log s$;*

(ii) *if there exists C' such that $c(q) \leq C'$ as $q \to \infty$, then $M = C'$.*

Then there exit at least $s - 1$ distinct monic sth-power free polynomials $h_i(x)$, $i = 1, 2, \ldots, s - 1$, in $F_q[x]$ of degree $\leq sn$ such that

$$\sum_{j=1}^{N} \chi(h_i(x_j)) = N$$

for each $i = 1, 2, \ldots, s - 1$.

Remark 1. Theorem 1 can be compared with Elliott's result on a lower bound of the least non-residue for a prime finite field.

Let χ be a nontrivial multiplicative character of F_q of exponent s. Let $s < q^{1/2}$. Define $A_{q,s} = \{f \in F_q[x]: f \notin (F_q[x])^s \text{ and } \deg f \leq s\}$. There exists a subset $B \subseteq F_q^*$ such that $f(B) \not\subseteq (F_q)^s$ for each $f \in A_{q,s}$, for instance $B = F_q^*$ by Weil's result.

Define $h(q, s)$ as the minimum of the cardinalities of the sets satisfying the property that $B \subseteq F_q^*$ and $f(B) \not\subseteq (F_q)^s$ for each $f \in A_{q,s}$. Then as a result of Theorem 1, $h(q, s) > d_s \log q$ for large q, where $d_s > 0$.

Define $B_{g(p,s)} = \{1, 2, \ldots, g(p, s)\} \subseteq F_p^*$. If $f(B_{g(p,s)}) \not\subseteq (F_p)^s$ for each $f \in A_{p,s}$, then $g(p, s) \geq h(p, s) > d_s \log p$ for large p where $d_s > 0$.

This result is similar to Elliott's result [6, 5]:

If $f(B_{g(p,s)}) \notin (F_p)^s$ for $f(x) = x$, then $g(p, s) > d_s \log p$ for infinitely many p where $d_s > 0$.

Note that our result holds for each sufficiently large prime number, while Elliott's result holds only for infinitely many prime numbers.

For the incomplete additive character sums we will prove the following theorems. Denote by ψ a nontrivial arbitrary additive character of F_q, i.e.,

$$\psi(x) = e^{2\pi i(\mathrm{tr}(\alpha x)/p)}, \qquad \text{where } \alpha \in F_q^*.$$

For simplicity we can restrict ourselves to the case $\alpha = 1$.

THEOREM 2. *Let $q = p^m$, p a prime number, $B = \{x_1, x_2, \ldots, x_N\} \subseteq F_q$ an arbitrary subset of F_q, and $0 < \varepsilon < 1/2\pi$. Let $1 \le n \le q^{1/2}$ be an integer satisfying*

$$n - \left[\frac{n}{p}\right] \ge \frac{N \log[(p-1)/p\varepsilon + 1]}{m \log p} + \frac{\log(2 + [(p-1)/p\varepsilon + 1]^{-N})}{m \log p}. \quad (4)$$

Then there exists a polynomial $f(x) \in F_q[x]$ such that $1 \le \deg f \le n$,

$$\mathrm{tr}(f(F_q)) \ne \{0\}, \qquad \textit{i.e., not identically zero on } F_q, \quad (5)$$

and

$$\left| \sum_{j=1}^{N} \psi(f(x_j)) \right| \ge N(1 - 2\pi\varepsilon). \quad (6)$$

For large p we can improve Theorem 2 by a stronger condition on f.

THEOREM 2′. *Let $q = p^m$, p a prime number, $B = \{x_1, x_2, \ldots, x_N\} \subseteq F_q$ an arbitrary subset of F_q, and $0 < \varepsilon < 1/2\pi - 1/p$. Let $n \ge 1$ be an integer satisfying*

$$\left[\frac{n+1}{m}\right] \ge \frac{N \log[(p + p\varepsilon)/(1 + p\varepsilon)]}{\log p} + \frac{\log(1 + [(p + p\varepsilon)/(1 + p\varepsilon)]^{-N})}{\log p}. \quad (7)$$

Then there exists a polynomial $f(x) \in F_q[x]$ *of degree* $\leq n$ *such that*

$$\operatorname{tr}(f(B)) \neq \{0\}, \qquad \textit{i.e., not identically zero on } B,$$

and

$$\left|\sum_{j=1}^{N} \psi(f(x_j))\right| \geq N\left(1 - 2\pi\left(\frac{1}{p} + \varepsilon\right)\right). \tag{8}$$

Moreover considering F_q *as an* F_p *vector space if* $x_1, x_2, \ldots, x_N$ *are collinear over* F_p (*i.e., there exists* $w \in F_q$ *such that* $x_j = wc_j$, $c_j \in F_p$ $j = 1, 2, \ldots, N$) *then* n *must satisfy*

$$n + 1 \geq \frac{N \log[(p + p\varepsilon)/(1 + p\varepsilon)]}{\log p} + \frac{\log(1 + [(p + p\varepsilon)]/(1 + p\varepsilon)]^{-N})}{\log p} \tag{9}$$

instead of inequality (7).

2. Notation and Lemmas

In this paper we will denote by F_q an arbitrary finite field of order $q = p^m$, p a prime number. $(\cdot/q)$ will represent the (generalized) Legendre symbol for F_q defined as follows:

$$\left(\frac{a}{q}\right) = \begin{cases} 0 & \text{if } a = 0 \\ 1 & \text{if } a \neq 0 \text{ and } a \text{ is a square in } F_q \\ -1 & \text{if } a \text{ is not a square in } F_q. \end{cases}$$

We will prove three lemmas. Lemma 1 is used for Theorem 1.

Lemma 1. *Let* $q = p^m$, p *a prime number*, $B = \{x_1, x_2, \ldots, x_N\} \subseteq F_q$ *an arbitrary subset of* F_q, *and* $1 \leq n < N \leq q$. *Moreover let* A_n *denote the set of polynomials in* $F_q[x]$ *having the following properties:*

(i) *the degrees of the polynomials are* $\leq n$,

(ii) *the polynomials have no root in* B,

(iii) *The polynomials are not of the form* $g(x)^2 h(x)$, *where* $g(x)$ *is a monic irreducible polynomial of degree* ≥ 1.

Then

$$|A_n| \geq q^{n+1}\left(\left(1-\frac{1}{q}\right)^N - K_q\right) + C_{q,N,n}, \tag{10}$$

where

$$0 \leq K_q \leq 5\log\frac{q}{q-1} \tag{11}$$

and

$$|C_{q,N,n}| \leq \binom{N}{n+1}. \tag{12}$$

Proof. Let E_1 be the set of all polynomials in $F_q[x]$ whose degrees are $\leq n$ and which have at least one root in B. Let E_2 be the set of all polynomials in $F_q[x]$ whose degrees are $\leq n$ and which have no root in B. Then using exclusion–inclusion arguments we have

$$|E_2| = q^{n+1} - |E_1|$$

and

$$|E_1| = \binom{N}{1} q^n - \binom{N}{2} q^{n-1} + \cdots + (-1)^{n+1}\binom{N}{n} q$$

so

$$\begin{aligned}|E_2| &= q^{n+1}\left(\left(1-\frac{1}{q}\right)^N - ((-1)^{n+1}\binom{N}{n+1}\frac{1}{q^{n+1}} + \cdots + (-1)^N\binom{N}{N}\frac{1}{q^N}\right)\right)\\ &= q^{n+1}\left(1-\frac{1}{q}\right)^N + C_{q,N,n},\end{aligned}$$

where

$$|C_{q,N,n}| \leq \binom{N}{n+1}.$$

Let S be the set of all polynomials of degree $\leq n$ and of the form $g(x)^2h(x)$, where $g(x)$ is a monic irreducible polynomial of degree ≥ 1. Let S_k be the set of all polynomials in S of the form $g_k(x)^2h(x)$, where g_k is a monic irreducible polynomial of degree k. Then

$$|S| \leq \sum_{k=1}^{[n/2]} |S_k|.$$

It is well-known that (see for example [1, p. 93]) the number of monic irreducible polynomials of degree k is

$$N_q(k) = \frac{1}{k} \sum_{d|k} \mu(d) q^{k/d} = \frac{1}{k} q^k c_k,$$

where μ is the Möbius function and

$$1 - \frac{q^k - q}{q^k(q-1)} \leq c_k \leq 1.$$

Then using exclusion–inclusion arguments

$$|S_k| \leq \binom{q^k/k}{1} q^{n+1-2k} + \cdots + (-1)^{[n/2k]+1} \binom{q^k/k}{[n/2k]} q^{n+1-[n/2k]2k},$$

where we used generalized binomial coefficients.

$$|S_k| \leq q^{n+1}\left(\frac{1}{kq^k}\right) + q^{n+1}R'_k, \qquad \text{where } |R'_k| \leq \frac{1}{kq^{2k}}$$

$$\sum_{k=1}^{[n/2]} |S_k| \leq q^{n+1} \log \frac{q}{q-1} + q^{n+1}R', \qquad \text{where } R' \leq 4 \log \frac{q^2}{q^2-1},$$

so

$$|S| \leq q^{n+1} 5 \log \frac{q}{q-1}.$$

Therefore

$$|A_n| \geq |E_2| - |S| \geq q^{n+1}\left(1 - \frac{1}{q}\right)^N + C_{q,N,n} - q^{n+1} 5 \log \frac{q}{q-1}$$
$$|A_n| \geq q^{n+1}\left(\left(1 - \frac{1}{q}\right)^N - K_q\right) + C_{q,N,n}. \quad \blacksquare \tag{13}$$

The set A_n includes the set of all of the irreducible polynomials of degree n. Stepanov used this subset instead of A_n. Since A_n has more elements our bound is slightly better than Stepanov's bound.

Lemma 2 and Lemma 3 are used for Theorem 2′. Lemma 2 is a special case of Lemma 3 with a better bound.

LEMMA 2. *Let $q = p^m$, p a prime number, $B = \{x_1, x_2, \ldots, x_N\} \subseteq F_q$ be given, and $1 \leq n < N \leq q$. Moreover let $x_1, x_2, \ldots, x_N$ be collinear over F_p. Define A_n as the set of all polynomials in $F_q[x]$ of degree $\leq n$. Let τ be the linear map between the F_p vector spaces*

$$\tau: A_n \to \prod_{i=1}^{N} F_p \tag{14}$$

with

$$\tau(f) = (\mathrm{tr}(f(x_1)), \mathrm{tr}(f(x_2)), \ldots, \mathrm{tr}(f(x_N))). \tag{15}$$

Then the rank of the corresponding matrix is $\geq n + 1$.

Proof. Each $f \in A_n$ can be written as $f(x) = \sum_{k=0}^{n} a_k x^k$, $a_k \in F_q$. There exists a normal basis $\{w_1, w_2, \ldots, w_m\} \subseteq F_q$ for F_q as a vector space over F_p such that $w_i = w^{p^{i-1}}$, $i = 1, 2, \ldots, m$ for some $w \in F_q$. Then

$$a_k = \sum_{j=1}^{m} \alpha_{k,j} w_j, \qquad \alpha_{k,j} \in F_p,$$

$$f(x) = \sum_{k=0}^{n} \sum_{j=1}^{m} \alpha_{k,j} w_j x^k.$$

By additivity of trace

$$\mathrm{tr}(f(x)) = \sum_{k=0}^{n} \sum_{j=1}^{m} \alpha_{k,j} \mathrm{tr}(w_j x^k).$$

Thus the matrix of this map is

$$A_{N,B} = \begin{bmatrix} \mathrm{tr}(w_1) & \cdots & \mathrm{tr}(w_m) & \mathrm{tr}(w_1x_1) & \cdots & \mathrm{tr}(w_mx_1) & \cdots & \cdots & \mathrm{tr}(w_1x_1^n) & \cdots & \mathrm{tr}(w_mx_1^n) \\ \mathrm{tr}(w_1) & \cdots & \mathrm{tr}(w_m) & \mathrm{tr}(w_1x_2) & \cdots & \mathrm{tr}(w_mx_2) & \cdots & \cdots & \mathrm{tr}(w_1x_2^n) & \cdots & \mathrm{tr}(w_mx_2^n) \\ \vdots & & \vdots & \vdots & & \vdots & & & \vdots & & \vdots \\ \mathrm{tr}(w_1) & \cdots & \mathrm{tr}(w_m) & \mathrm{tr}(w_1x_N) & \cdots & \mathrm{tr}(w_mx_N) & \cdots & \cdots & \mathrm{tr}(w_1x_N^n) & \cdots & \mathrm{tr}(w_mx_N^n) \end{bmatrix}$$

$$\begin{bmatrix} \mathrm{tr}(w_1) & \mathrm{tr}(w_jx_1) \\ \mathrm{tr}(w_1) & \mathrm{tr}(w_jx_2) \end{bmatrix} \quad \text{is a submatrix of } A_{N,B}.$$

$\mathrm{tr}(w_j) \neq 0$ for any $j = 1, 2, \ldots, m$. Moreover for some j, $1 \leq j \leq m$, $\mathrm{tr}(w_j(x_2 - x_1)) \neq 0$, if $x_2 \neq x_1$; since otherwise $\mathrm{tr}(\alpha(x_2 - x_1)) = 0$ for each $\alpha \in F_q$ so $\mathrm{tr}(\beta) = 0$ for each $\beta \in F_q$. Then rank $A_{N,B} \geq 2$. Define $A_{N,B}(j_1, j_2, \ldots, j_n)$, $1 \leq j_i \leq m$, $i = 1, 2, \ldots, n$, which is a submatrix of $A_{N,B}$, as below:

$$A_{N,B}(j_1, j_2, \ldots, j_n) = \begin{bmatrix} \mathrm{tr}(w_1) & \mathrm{tr}(w_{j_1}x_1) & \mathrm{tr}(w_{j_2}x_1^2) & \cdots & \mathrm{tr}w_{j_n}x_1^n) \\ \mathrm{tr}(w_1) & \mathrm{tr}(w_{j_1}x_2) & \mathrm{tr}(w_{j_2}x_2^2) & \cdots & \mathrm{tr}(w_{j_n}x_2^n) \\ \vdots & \vdots & \vdots & & \vdots \\ \mathrm{tr}(w_1) & \mathrm{tr}(w_{j_1}x_{n+1}) & \mathrm{tr}(w_{j_2}x_{n+1}^2) & \cdots & \mathrm{tr}(w_{j_n}x_{n+1}^n) \end{bmatrix}.$$

Using the facts that

(i) $x_1, x_2, \ldots, x_N$ are collinear over F_p,

(ii) $A_{N,B}(j_1, j_2, \ldots, j_n)$ is similar to the Vandermonde matrix, we can bring $A_{N,B}(j_1, j_2, \ldots, j_n$ into an equivalent form $\overline{A}_{N,B}(j_1, j_2, \ldots, j_n)$, which is

$$\overline{A}_{N,B}(j_1, j_2, \ldots, j_n)$$

$$= \begin{bmatrix} \mathrm{tr}(w_1) & * & \cdots & * \\ 0 & \mathrm{tr}(w_{j1}(x_2 - x_1)) & \cdots & * \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \mathrm{tr}(w_{j_n}(x_n - x_{n-1})(x_{n-1} - x_{n-2}) \cdots (x_2 - x_1)) \end{bmatrix},$$

where $*$ represents a don't care entry. Since $x_1 \neq x_{j_2}$ if $j_1 \neq j_2$, $\overline{A}_{N,B}(j_1, j_2, \ldots, j_n)$ is nonsingular. Therefore rank $\tau \geq n + 1$. ■

LEMMA 3. *Let $q = p^m$, p a prime number, $B = \{x_1, x_2, \ldots, x_N\} \subseteq F_q$ be given and $1 \le n < N \le q$. Define A_n as the set of all polynomials in $F_q[x]$ of degree $\le n$. Let τ be the linear map between the F_p vector spaces*

$$\tau: A_n \to \prod_{i=1}^{N} F_p \tag{16}$$

with

$$\tau(f) = (\mathrm{tr}(f(x_1)), \mathrm{tr}(f(x_2)), \ldots, \mathrm{tr}(f(x_N))). \tag{17}$$

Then the rank of the corresponding matrix is $\ge [(n+1)/m]$.

Proof. We know $f(x) = \sum_{k=0}^{n} \sum_{j=1}^{m} \alpha_{k,j} w_j x^k$, where $\alpha_{k,j} \in F_p$, $w_j = w^{p^{j-1}}$ forming a normal basis:

$$\mathrm{tr}(f(x)) = f(x) + f(x)^p + \cdots + f(x)^{p^{m-1}} \qquad \text{and} \qquad (f(x))^{p^\nu}$$
$$= \sum_{k=0}^{n} \sum_{j=1}^{m} \alpha_{k,j} w_j^{p^\nu} x^{kp^\nu}, 0 \le \nu \le m-1.$$

Define $\xi_{i,\nu} = x_i^{p^\nu}$, $i = 1, 2, \ldots, N$. By normality of the basis, $w_j^{p^\nu} = w_{j+\nu}$. Therefore $f \in \mathrm{Ker}(\tau)$ if and only if

$$\mathrm{tr}(f(x_i)) = \sum_{\nu=0}^{m-1} \sum_{k=0}^{n} \sum_{j=1}^{m} \alpha_{k,j} w_{j+\nu} \xi_{i,\nu}^k = 0 \qquad \text{for each } 1 \le i \le N. \tag{18}$$

We can write the system (18) in matrix notation as

$$(\tilde{A}_{N,B})_{N \times (n+1)m^2} (\tilde{b}_{N,B})_{(n+1)m^2 \times 1} = (0)_{N \times 1}, \tag{19}$$

where

$$\tilde{A}_{N,B} = \begin{bmatrix} A_{1,0} & A_{1,1} & \cdots & A_{1,m-1} \\ A_{2,0} & A_{2,1} & \cdots & A_{2,m-1} \\ \vdots & \vdots & & \vdots \\ A_{N,O} & A_{N,1} & \cdots & A_{N,m-1} \end{bmatrix}, \qquad \tilde{b}_{N,B} = \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{m-1} \end{bmatrix}$$

with

$$A_{i,v} = \left[\overbrace{1 \cdots 1}^{m \text{ times}} \quad \overbrace{\xi_{i,v} \cdots \xi_{i,v}}^{m \text{ times}} \quad \cdots \quad \overbrace{\xi_{i,v}^n \cdots \xi_{i,v}^n}^{m \text{ times}} \right],$$

$$b_v = \begin{bmatrix} \alpha_{0,1} w_{1+v} \\ \alpha_{0,2} w_{2+v} \\ \vdots \\ \alpha_{0,m} w_{m+v} \\ \alpha_{1,1} w_{1+v} \\ \alpha_{1,2} w_{2+v} \\ \vdots \\ \alpha_{1,m} w_{m+v} \\ \vdots \\ \alpha_{n,1} w_{1+v} \\ \alpha_{n,2} w_{2+v} \\ \vdots \\ \alpha_{n,m} w_{m+v} \end{bmatrix}.$$

There is a natural isomorphism between F_P vector spaces A_n and $\prod_{i=1}^{(n+1)m} F_p$. Therefore $\mathrm{Ker}(\tau) = \{(\alpha_{0,1}, \ldots, \alpha_{0,m}, \alpha_{1,1}, \ldots, \alpha_{1,m}, \ldots, \ldots, \alpha_{n,1}, \ldots, \alpha_{n,m}) \in \prod_{i=1}^{(n+1)m} F_p : \tilde{b}_{N,B}$ formed with this vector satisfies (18)$\}$.

But we can observe that in $\tilde{b}_{N,B}$ for each $\alpha_{k,j}$ there exist m entries as $\alpha_{k,j} w_l$, $1 \le l \le m$. For $v = 0$ we have a submatrix $A^*_{N,B}$ of $\tilde{A}_{N,B}$

$$A^*_{N,B} = \begin{bmatrix} 1 & \xi_{1,0} & \cdots & \xi_{1,0}^n \\ 1 & \xi_{2,0} & \cdots & \xi_{2,0}^n \\ \vdots & \vdots & & \vdots \\ 1 & \xi_{n+1,0} & \cdots & \xi_{n+1,0}^n \end{bmatrix} = \begin{bmatrix} 1 & x_1 & \cdots & x_1^n \\ 1 & x_2 & \cdots & x_2^n \\ \vdots & \vdots & & \vdots \\ 1 & x_{n+1} & \cdots & x_{n+1}^n \end{bmatrix},$$

which is a Vandermonde matrix.

Therefore $\dim\{\tilde{b}_{N,B} \in \prod_{i=1}^{(n+1)m^2} F_p : \tilde{b}_{N,B} \text{ satisfying (18)}\} \leq (n+1)m^2 - (n+1)$. Since there is an m to 1 map from this kernel $\in \prod_{i=1}^{(n+1)m^2} F_p$ to $\mathrm{Ker}(\tau) \in \prod_{i=1}^{(n+1)m} F_p$, we have $\dim(\mathrm{Ker}(\tau)) \leq -[-(n+1)m + (n+1)/m]$. Therefore

$$\mathrm{rank}(\tau) \geq (n+1)m + \left[-(n+1)m + \frac{n+1}{m}\right] = \left[\frac{n+1}{m}\right]. \quad \blacksquare$$

3. Proof of Theorem 1

First we will prove Theorem 1 for the generalized Legendre symbol in Proposition 1.

Proposition 1. *Let $q = p^m$, p an odd prime number, $B = \{x_1, x_2, \ldots, x_N\} \subseteq F_q$ an arbitrary subset of F_q. Assume $N = c(q)\log q$ and $n \geq 1$ is an integer satisfying*

$$n \geq \frac{N\log 2}{\log q} - \frac{N\log(1-1/q) + \log(1 - K_q(1-1/q)^{-N})}{\log q} + \frac{\log(1-2^{-N})}{\log q} + R_{N,q}, \tag{20}$$

where

$$0 \leq K_q \leq 5\log\frac{q}{q-1} \tag{21}$$

and

$$|R_{N,q}| \leq \left(M\frac{\log q}{q}\right)^2 \frac{1}{(1-1/q)^N - K_q} \tag{22}$$

and also where

(i) *if $c(q) \to \infty$ as $q \to \infty$, then $M = e/\log 2$;*

(ii) *if there exists C' such that $c(q) \leq C'$ as $q \to \infty$, then $M = C'$.*

Then there exists a monic square free polynomial $f(x)$ in $F_q[x]$ of degree $\leq 2n$ such that

$$\sum_{j=1}^{N} \left(\frac{f(x_j)}{q}\right) = N,$$

where $(\cdot/q)$ is the generalized Legendre symbol.

Proof. Let A_n^* be the set of all monic polynomials in A_n, which is the set defined in Lemma 1. Then

$$|A_n^*| = \frac{|A_n|}{q} \geq q^n \left(\left(1 - \frac{1}{q}\right)^N - K_q\right) + \frac{C_{q,N,n}}{q}.$$

For each polynomial in A_n^* assign an *N-tuple* as follows:

$$f_i \in A_n^* \mapsto \gamma_i \in \prod_{i=1}^{N} \{-1, 1\}$$

$$\gamma_i = \left(\left(\frac{f_i(x_1)}{q}\right), \left(\frac{f_i(x_2)}{q}\right), \ldots, \left(\frac{f_i(x_N)}{q}\right)\right).$$

If $|A_n^*| \geq 2^N + 1$, then there exist at least two equal *N-tuples* $\gamma_1 = \gamma_2$ where $f_1 \not\equiv f_2$. Define f as $f = f_1 f_2$. Since f_i is a square-free polynomial $i = 1, 2$, f is not a square polynomial. Moreover $(f(x_j)/q) = 1$ for each $j = 1, 2, \ldots, N$. So

$$\sum_{j=1}^{N} \left(\frac{f(x_j)}{q}\right) = N \qquad \text{and} \qquad \deg f \leq 2n$$

and

$$2^N + 1 \leq q^n \left(\left(1 - \frac{1}{q}\right)^N - K_q\right) + \frac{C_{q,N,n}}{q} \leq |A_n^*|,$$

whenever

$$n \geq \frac{N \log 2}{\log q} - \frac{N \log(1 - 1/q) + \log(1 - K_q(1 - 1/q)^{-N})}{\log q} + \frac{\log(1 + 2^{-N})}{\log q}$$
$$+ \log\left(1 + \frac{C_{q,N,n}}{q^{n+1}((1 - 1/q)^N - K_q)}\right).$$

If $c(q) \leq C'$, then $\binom{N}{n+1} \leq N^{n+1}/(n+1)! \leq (C' \log q)^{n+1}$.

If $c(q) \to \infty$ as $q \to \infty$, then using Stepanov's result $n + 1 \to \infty$ as $q \to \infty$ and

$$n \geq \frac{(N+1)\log 2}{\log q} + 1 \Rightarrow \frac{N}{n+1} \leq \frac{\log q}{\log 2}.$$

Now using Stirling's formula for $\binom{N}{n+1}$, i.e.,

$$\log N! = \left(N + \frac{1}{2}\right)\log N - N + C + O\left(\frac{1}{N}\right),$$

$$\text{where } C = \frac{1}{2}\log 2\pi \text{ as } q \to \infty,$$

we get

$$\binom{N}{n+1} = \left(\frac{N}{n+1}\right)^{n+1} \frac{1}{\sqrt{n+1}}\, e^{(n+1)(1-(2n+1)/2N)(1-O((n+1)/N))-C+O(1/(n+1)+1/(N-n-1))}.$$

So

$$\binom{N}{n+1} \leq \left(\frac{\log q}{\log 2}\right)^{n+1} e^{n+1} = \left(\frac{e}{\log 2}\log q\right)^{n+1}.$$

Thus $|C_{q,N,n}| \leq (M \log q)^{n+1}$, where if $c(q)$ is bounded by C', then $M \geq C'$; else $M = e/\log 2$. But

$$\left|\log\left(1 + \frac{C_{q,N,n}}{q^{n+1}((1-1/q)^N - K_q)}\right)\right| \leq \left(M\frac{\log q}{q}\right)^2 \frac{1}{(1-1/q)^N - K_q}.$$

Thus

$$n \geq \frac{N\log 2}{\log q} - \frac{N\log(1-1/q) + \log(1 - K_q(1-1/q)^{-N})}{\log q} + \frac{\log(1-2^{-N})}{\log q} + R_{N,q},$$

where

$$|R_{N,q}| \le \left(M\frac{\log q}{q}\right)^2 \frac{1}{(1-1/q)^N - K_q}.$$

If $f(x)$ is square-free, then we are done. Otherwise $f(x) = f'(x)(g(x))^2$, where $f'(x)$ is a square-free polynomial. Thus deg $f'(x) \le$ deg $f(x)$ and $\chi(f'(x)) = \chi(f(x))$ for each $x \in B$. Therefore $f'(x)$ satisfies the conditions. ■

This proposition easily extends to the case of general multiplicative characters.

Proof of Theorem 1. Assume f_1 and f_2 are distinct polynomials of degree $\le n$, not vanishing in B and they are not of the form $g(x)^2h(x)$, where $g(x)$ is a monic irreducible polynomial, i.e., square-free. Then

$$f_1^{i_1} f_2^{s-i_1} \equiv f_1^{i_2} f_2^{s-i_2} \Leftrightarrow f_1^{i_1-i_2} \equiv f_2^{i_1-i_2} \Leftrightarrow i_1 = i_2$$

by unique factorization. Let A_n^* be the set defined in the proof of Proposition 1. We know

$$|A_n^*| = \frac{|A_n|}{q} \ge q^n \left(\left(1-\frac{1}{q}\right)^N - K_q\right) + \frac{C_{q,N,n}}{q},$$

where

$$0 \le K_q \le 5\log\frac{q}{q-1} \qquad \text{and} \qquad |C_{q,N,n}| \le \binom{N}{n+1}.$$

Thus if

$$q^n \left(\left(1-\frac{1}{q}\right)^N - K_q\right) + \frac{C_{q,N,n}}{q} \ge s^N + 1 \tag{23}$$

there exist at least two polynomials $f_1 \not\equiv f_2$ such that

$$\chi(f_1(x_j)) = \chi(f_2(x_j)) \qquad \text{for each } j = 1, 2, \ldots, N.$$

Define $h_i = f_1^i f_2^{s-i}$, $i = 1, 2, \ldots, s-1$. Then

$$\chi(h_i(x_j)) = \chi(f_1^i(x_j))\chi(f_2^{s-i}(x_j)) = \chi(f_2^s(x_j)) = 1$$
$$\text{for each } j = 1, 2, \ldots, N.$$

Moreover $h_{i_1} \not\equiv h_{i_2}$ if $i_1 \neq i_2$, $i_l = 1, 2, \ldots, s-1$. Therefore if the inequality (23) is satisfied, then there exist $(s-1)$ distinct monic polynomials satisfying the condition which are not in $(F_q[x])^s$. The inequality is satisfied whenever

$$n \geq \frac{N \log s}{\log q} - \frac{N \log(1-1/q) + \log(1 - K_q(1-1/q)^{-N})}{\log q} + \frac{\log(1+s^{-N})}{\log q} + \log\left(1 + \frac{C_{q,N,n}}{q^{n+1}((1-1/q)^N - K_q)}\right).$$

If $c(q) \leq C'$, then $\binom{N}{n+1} \leq N^{n+1}/(n+1)! \leq (C' \log q)^{n+1}$.

If $c(q) \to \infty$ as $q \to \infty$, then we can extend Stepanov's result for any multiplicative character of exponent s such that if $s^N + 1 \leq q^n/2n$ there are $s-1$ different nontrivial polynomials which are mapped to 1 at each point in B. This implies

$$\frac{N}{n+1} \leq \frac{N \log q}{N \log s + \log(1+s^{-N}) + \log(2n) + \log s} \leq \frac{\log q}{\log s}.$$

By using Stirling's formula $\binom{N}{n+1} \leq (\log q/\log s)^{n+1} e^{n+1} = ((e/\log s) \log q)^{n+1}$. So we can take $M = e/\log s$. Thus

$$\left|\log\left(1 + \frac{C_{q,N,n}}{q^{n+1}((1-1/q)^N - K_q)}\right)\right| \leq \left(M \frac{\log q}{q}\right)^2 \frac{1}{(1-1/q)^N - K_q}.$$

Similar to the proof of Proposition 1, if $h_i(x)$ is not sth-power free, then $h_i(x) = h_i'(x)(g_i(x))^s$, where $h_i'(x)$ is sth-power free and satisfies the conditions for $i = 1, 2, \ldots, (s-1)$. ■

4. Proof of Theorems 2 and 2′

Proof of Theorem 2. Let $1 \leq n \leq q^{1/2}$ be an integer. Define $k = [n/p]$. Let C be the set of all polynomials f in $F_q[x]$ which are not identically zero having the property that $1 \leq \deg f \leq n$ and the coefficients of x^{pi} are zero for each $i = 0, 1, \ldots, k$. Namely $C = \{(a_1 x + \cdots a_{p-1}x^{p-1}) + (a_{p+1} x^{p+1} + \cdots + a_{2p-1}x^{2p-1}) + \cdots + (a_{kp+1}x^{kp+1} + \cdots + a_n x^n) \mid a_i \in F_q$, not each a_i is zero$\}$.

Then the cardinality of C is $|C| = q^{n-[n/p]} - 1$. If $f_1, f_2 \in C$ and $f_1 \neq f_2$, then $(\deg(f_1 - f_2), p) = 1$. So since $\deg(f_1 - f_2) \leq n \leq q^{1/2}$ by Weil's theorem for additive characters (see for example [1], Theorem 5.28, p. 223]) $\mathrm{tr}(f_1 - f_2)(F_q) \neq \{0\}$.

Let $K = [(p-1)/p\varepsilon + 1]$. Define $U_i = [(i-1)\varepsilon, i\varepsilon)$, $1 \le i \le K$ as an interval in $[0, (p-1)/p + \varepsilon)$ and $(p-1)/p \in U_K$. $U_i \cap U_j = \varnothing$ if $i \ne j$. For each $f \in C$ define an N-tuple as follows:

$$\Gamma(f) = (l_1, l_2, \ldots, l_N), \quad \text{where } \frac{\operatorname{tr}(f(x_i))}{p} \in U_{l_i}, l_i \in 1, 2, \ldots, K, \text{ and } 1 \le i \le N.$$

There are K^N distinct values on the image of Γ. If $|C| \ge K^N + 1$ there are at least two distinct polynomials f_1, f_2 in C such that

$$\left|\frac{\operatorname{tr}(f_1 - f_2)(x_i)}{p}\right| \le \varepsilon \quad \text{for each } i = 1, 2, \ldots, N.$$

Let $f = f_1 - f_2$. Then

$$\left|\sum_{i=1}^{N} \psi(f(x_i))\right| = \left|\sum_{i=1}^{N} e^{2\pi i(\operatorname{tr}(f(x_i))/p)}\right| \ge \sum_{i=1}^{N} \operatorname{Re}(e^{2\pi i(\operatorname{tr}(f(x_i))/p)})$$
$$= \sum_{i=1}^{N} \cos\left(2\pi \frac{\operatorname{tr}(f(x_i))}{p}\right).$$

Using $\cos x = \cos |x| \ge 1 - |x|$

$$\cos\left(2\pi \frac{\operatorname{tr}(f(x_i))}{p}\right) \ge 1 - 2\pi\varepsilon.$$

Thus $|\sum_{i=1}^{N} \psi(f(x_i))| \ge N(1 - 2\pi\varepsilon)$.

We know $|C| = q^{n-[n/p]} - 1$. Thus whenever $K^N + 1 \le q^{n-[n/p]} - 1$ the existence of such f is guaranteed. But this means

$$n - \left[\frac{n}{p}\right] \ge \frac{N \log([(p-1)/p\varepsilon + 1]) + \log(2 + [(p-1)/p\varepsilon + 1]^{-N})}{m \log p}. \quad \blacksquare$$

Proof of Theorem 2′. Let A_n be the set of all polynomials in $F_q[x]$ whose degree is $\le n$. Let $f_1 \in A_n$. Denote by k the $\dim(\operatorname{Ker}(\tau))$ and let $r = \operatorname{rank}(\tau)$, where τ is the map defined in lemmas. Then define

$$S_1 = \{g_1 \in A_n : \operatorname{tr}((g_1 - f_1)(x_i)) = 0 \text{ for each } i = 1, 2, \ldots, N\} \subseteq A_n.$$

Let $f_2 \in A_n \backslash S_1$. Define

$$S_2 = \{g_2 \in A_n : \mathrm{tr}((g_2 - f_2)(x_i) = 0 \text{ for each } i = 1, 2, \ldots N\} \subseteq A_n.$$

Let $f_j \in A_n \backslash \bigcup_{i=1}^{j-1} S_i$ for $j = 3, 4, \ldots, m$, where

$$S_j = \{g_j \in A_n : \mathrm{tr}((g_j - f_j)(x_i) = 0 \text{ for each } i = 1, 2, \ldots N\} \subseteq A_n.$$

Thus $|S_j| = p^k$ for $j = 1, 2, \ldots, l$ and $l = p^r$. Define $C = \{f_1, f_2, \ldots, f_l\} \subseteq A_n$. $|C| = p^r$ and $r \geq [(n+1)/m]$ (resp. $n+1$ if $\{x_1, x_2, \ldots, x_N\}$ are collinear) by Lemma 3 (resp. Lemma 2).

Let $K = [(p + p\varepsilon)/(1 + p\varepsilon)]$. Define $U_i = [(i-1)(1/p + \varepsilon), i(1/p + \varepsilon))$, $1 \leq i \leq K$ as an interval in $[0, 1 + \varepsilon)$ and $(p-1)/p \in U_K$. By similar arguments as in the proof of Theorem 2, if $K^N + 1 \leq p^r \leq p[(n+1)/m]$ (resp. p^{n+1}) there exists a polynomial f of degree $\leq n$ such that

$$\left| \sum_{i=1}^{N} \psi(f(x_i)) \right| \geq N\left(1 - 2\pi\left(\frac{1}{p} + \varepsilon\right)\right).$$

But this means

$$\left[\frac{n+1}{m}\right] (\text{resp. } n+1) > \frac{N \log[(p + p\varepsilon)/(1 + p\varepsilon)] + \log(1 + [(p + p\varepsilon)/(1 + p\varepsilon)]^{-N})}{\log p}.$$

Moreover $\mathrm{tr}(f(B)) \neq \{0\}$ by Lemma 3 (resp. Lemma 2). ■

Acknowledgment

I thank S. A. Stepanov for his excellent guidance, comments, and suggestions. He introduced me to the problem and helped in all steps by his marvelous ideas. I also thank the referee for suggestions.

References

1. R. Lidl and H. Niederreiter, "Finite Fields," Encyclopedia of Mathematics and Its Applications, Vol. 20, Cambridge Univ. Press, Cambridge, UK, 1984.
2. W. M. Schmidt, "Equations over Finite Fields An Elementary Approach," Lecture Notes in Mathematics, Vol. 536, Springer-Verlag, New York/Berlin, 1976.

3. S. A. Stepanov, The arithmetic of algebraic curves, in ''Monographs in Contemporary Mathematics,'' Plenum Publishing Corporation, New York, 1994.
4. A. A. Karatsuba, Lower bounds for character sums of polynomials, *Mat. Zametki* **14** (1973), 67–72; English transl. in *Math Notes* **14** (1973).
5. K. K. Norton, ''Bounds for sequences of consecutive power residues, I,'' Proceedings of Symposia in Pure Mathematics, Vol. 24, pp. 213–220, Am. Math. Soc., Providence, RI, 1973.
6. P. D. T. A. Elliott, ''Some notes on k-th power residues, *Acta Arith.* **14** (1967/68), 153–162.
7. D. A. Mit'kin, Lower bounds for sums of Legendre Symbols and trigonometric sums, *Usp. Mat. Nauk* **30** (1975), 185–214 [in Russian].
8. S. A. Stepanov, On lower estimates of incomplete character sums of polynomials, *Proc. Steklov Inst. Math.* **1** (1980), 187–189.
9. A. Weil, Numbers of solutions of equations in finite fields, *Bull. Amer. Math. Soc.* **55** (1949), 497–508.